INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

TRACKING DIGITAL DEVICES AND COLLECTING EVIDENCES FOR CYBER INVESTIGATION

G.Siddharth[1], E. Saravanan[2]

[1]M.Tech Information Security and Cyber Forensics
Dr. M.G.R. Educational and Research Institute University, Maduravoyl, Chennai, TN-95
[2]Professor, Department of CSE/IT
Dr. M.G.R. Educational and Research Institute University, Maduravoyl, Chennai, TN-95
gsiddharth29@gmail.com

Abstract

The development of technologies is very consistent since the 21st century. Computers started to play a big role in every organization and every individual depends on it and uses them almost every day. Companies store sensitive information's in computer and individuals store their personal data's like photos, videos, and other personal information's on their computers. Initially it was difficult for transferring data's from one system to another but due to the immense growth of technology different types of external or removable storage devices came into existence like USB pen drives, Flash Drives, Memory Cards, CD's, DVD's etc. These devices have become very vulnerable for getting stolen or misplaced. In this paper, we have given solution to overcome the above mentioned problem of data and device theft by tracking the devices constantly and collect all important evidences from the Computers in which they are plugged in and these can be very crucial for giving verdict in a court of law.

Keywords— Information Security, Digital Forensics, Device Security

1. Introduction

As we know Charles Babbage invented the first programmable computer in 19th century and it led to further alteration and enhancement by few other inventors like Sir William Thomson and James Thomson to build the computer intelligent. Later the modern computer was designed and invented by scientist Alan Turing which was accompanied by the work of Konrad Zuse, Tommy Flowers and many more.

The generation of the computer was like; first general purpose computing device then analog computers, modern computer, electrochemical computers, electronic programmable computer, stored program computer, transistor computer, then came the advanced computers with the help on integrated circuits and microprocessors. The design, size, performance and intelligence of the computers have been growing drastically from the 19th century till date. Computers are being used in almost all the industries like in Hospitals, IT firms, Government companies and in almost in every house people use it as it can be bought in affordable price now a days.

The operating systems were then developed in 1950's where many unique operating systems to perform only specific task was developed and later sophisticated operating systems like Windows and Linux were

developed. In today's era, Windows is the largely used operating system than any other operating system. People use computers for many purposes like to do business, build documents, play games, to store photos, videos, and other sensitive information concerning their privacy. The storage medium was initially the primary storage device which is the Hard-disk and later on by the growing technologies many kinds of secondary storage devices were designed to make storage and data transfer and portability easier. Such devices are for example floppy disks, portable hard disks, CD's and DVDs, memory sticks or pen drives, flash memory cards.

As and when the computers are started to being used in many places the threats and vulnerabilities also came into existence. There are lots of threats that can occur by using computers and one of the main threats is the storage devices being stolen. In many industries or organization people store lots of important data's and sensitive information on their removable storage device and think that they have it secured. People often keep such removable device near to their computers or with them in their pockets or bags. So the risk factor of the device being stolen or misplaced is very high and the impact of the consequence is also high when it contains confidential data's. There is no possibility to find such kinds of devices once stolen or misplaced. For that we need to find some solution to hold the device and data secured and in case if someone stole the device on purpose we need some procedure to find the criminal who stole it and also get back the device.

For the above stated scenario, we provide a solution to track the device and collect evidences for convicting the criminal who stole it. The solution includes process to register the device with the end user's computer and keep a constant log whenever he uses it. If someone steels the device and plug it into an unregistered computer the device collects all the fingerprints of that computer or laptop and sends all the information to the owner of the device which supports as an important evidence for filing a cybercrime case against the criminal.

2. Evolution of storage device

From the beginning of mankind, man tried to find a way to store information for the upcoming generations. The history of information storage goes back to pre-historic times where mankind used red and yellow ochre, hematite, manganese oxide and charcoal to paint information about their life on rock walls, caves and ceilings.

2.1 Late BC:

In Ancient Egypt "Papyrus", which is an early form of paper, was used to store information. It remained in use until 800 AD, when it was replaced by cheaper paper. Before then, the use of parchment and vellum had replaced papyrus in many areas as they are much more durable. The Chinese ordinarily wrote documents on bamboo. Also silk, bones, shells and ivory were used, later bronze, iron, gold, silver, tin, jade, stone and clay. In India palm leaves were used for storing information. In the late 4th millennium BC Sumerians created the cuneiform script that was drawn on clay tablets. Finally, sometime between 150 BC and 105 AD paper was invented. These kinds of storage medium held lot of valuable informations for several centuries and now they are preserved in museum's.

2.2 Medieval to the 17th Century:

In medieval England, the "tally stick" was a wide spread mnemonic device of the Exchequer for the collection of taxes by local sheriffs. Its origin goes back to the Stone Age. Also the Incas (ca. 1400-1632 AD) had a kind of "memory aid" which was the Quipu and consisted of knots. In 1440 AD the invention of printing by Gutenberg was really a milestone in the history of information storage. After the 17th century inventions that usually need some kind of aid to read the information from a particular storage were made. Some examples of that are; the punch card, punched tape, Phonograph, magnetic tape, magnetic drum, telegraph and the selection tube.

2.3 19th Century:

In 1956, IBM invented the hard disk with a size of 5 MB, which was a fantastic innovation of that period. In the years between 1950 and 1980 some storage devices where build that nowadays hardly anyone would remember, for example the bubble memory or the twister memory. On the other hand there were some technologies introduced that were very important for the development of the computer industry and some of these technologies are still in use today. One of these technologies was the first memory disk, called the floppy disk, invented by Alan Shugart at IBM in 1971. It was considered as a revolutionary device for transporting data from one computer to another. Floppy disks were not able to store as much data as hard disks, but they were much cheaper and more flexible. This invention was also the end for punch cards. At the beginning of the 1980s the first optical devices, the CD and the CD-ROM were released. In the middle of the 1990s these and several other optical devices started to get more and more important and they are widely used today. Exactly at

that time the first electronic devices were developed. These devices, e.g. Compact Flash Cards, Memory Sticks etc., are very small but they can store a lot of data and so they find their use in digital cameras, PDAs etc. But the development of the magnetic devices did not stop, several new technologies like the Advanced Intelligent Tape were introduced and the main hard disc in a pc is still based on magnetic technology.

2.4 21st Century:

In the 21st century, the development of the technologies led us from the widely used optical devices to the laser device up to holographic memories. In 2003 the first blue-laser based disc, the Blue-ray disc, was released and the first PC drives came out in 2006. Several other "versions" of the DVD, e.g. HD-DVD have been released since then, all modified to store more and more data and to gain faster access.

2.5 Latest Technology:

The latest prevailing and fast growing technology is the cloud storage where huge volumes of data's are stored virtually in data centres around the world. It is Made up of many distributed resources, but still acts as one. Many other developments in storage devices are the pen drives and external hard disks with several terabytes of storage capacity which could hold data's for millions of years.

3. Proposed Concept

Any storage device like pen drive, flash drive, memory card normally when inserted in a system, the system reads the content on the storage device, loads the drive and then displays the drive in the computer. The system does not know whether the content on the pen drive should be displayed or not, it just does its work by loading the device on the system. Now a day's people store sensitive information or other personal details on storage devices like CD's, DVD's, pen drives etc., which is secure only when it is with them. If someone steals the device they could view the contents on the device easily. Till now protection for such devices is to have a folder lock or encrypt the files on the device, but these techniques can be easily broken by anyone who knows how to crack them and they are even easier for a hacker and also such devices once stolen cannot be tracked. And so the owner loses his data with the device. My system overcomes this issue by providing solution for tracking the device.

3.1 Architecture:

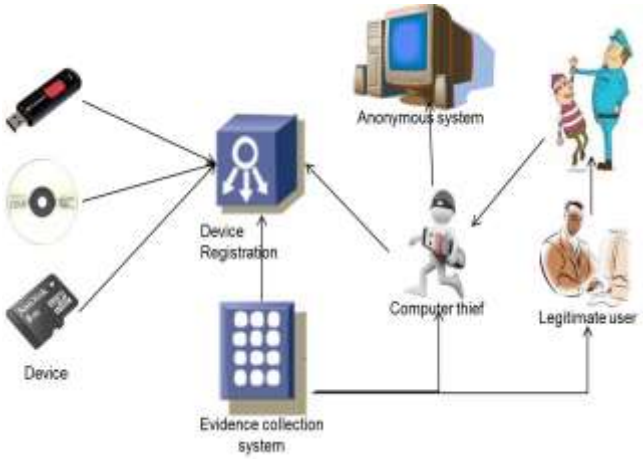

Figure 1: System Architecture

The overall working of the system is depicted by the above system architecture. The user first wants to register his computer with the device using my device tracking system which will be embedded onto the hardware of the storage device in a ROM memory. The user needs to sign up a new account in the system and register his unique identification numbers and features of his computers hardware. The details get stored on the registered device. Each and every time the device is plugged into a computer or a laptop the device automatically compares the details stored on the device with the computer and if even one attribute does not match, the device collects certain unique information from the system like: MAC Address, IP Address, User Accounts details, Hostname, Bios Id, OS Fingerprint etc., and automatically sends the collected informations through mail to the owner of the device.

There are three modules in my system and they are:

- ❖Device Registration,
- ❖Evidence Collection &
- ❖Automatic Mail Transfer

3.2 Device Registration:

This is the basic and the first part of the system where the owner of the device registers his hardware details with the device so that the device could be used only in his system and the data's could be viewed only in his system. The registered information gets stored in an encrypted format on the device. Also we have an online website which offers services like user registration which holds a record of all the events taking place.

3.3 Evidence Collection:

The second main feature of my system is the evidence collection system which collects unique informations from the computer when the device is being plugged on a different system. The device collects very important informations like:

a) MAC Address: A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are also known as hardware addresses or physical addresses. MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats: MM:MM:MM:SS:SS:SS (or) MM-MM-MM-SS-SS-SS. The first half of a MAC address contains the ID number of the adapter manufacturer. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.

b) IP Address: An IP address is a binary number that uniquely identifies computers and other devices on a TCP/IP network. There are two standards for IP addresses: IP Version 4 (IPv4) and IP Version 6 (IPv6). IPv4 uses 32 binary bits to create a single unique address on the network. IPv6 uses 128 binary bits to create a single unique address on the network. An IP address can be either dynamic or static. A static address is unique and a dynamic address is common.

c) Other details which are collected are BIOS id, OS details etc.

The above mentioned details are some of the backbone of a computer for identifying it uniquely. These informations are helpful in identifying stolen storage devices or memory cards or CD/DVD's etc. Whenever these devices are inserted in an anonymous computer the device gathers all these important informations for tracking them through an ISP or System manufacture.

3.4 Automatic Mail Transfer:

This is the critical feature of the system which pushes the collected or gathered evidences from the anonymous computer to the rightful owner of the device and also to our system website from where the complaint can be launched directly to the Cyber Cell for tracking the criminal and getting back the stolen device. These evidences are logs created at the time when the device is attempted to plug into a different computer. This can be considered as important evidence in the court of low for prosecuting a criminal for cybercrime.

4. Security Analysis

In this chapter we discuss about the security of our system comparing with the previously available system. In our system, the three different modules adds a layer of security to the data in the device and also to the device itself on its own. In addition to that we provide a password authentication to view the files and folders on the pen drive, we use DES encryption and decryption to secure the registered system information on the device from others viewing and modifying it. We compare our system with the existing technology on five bases:

I. Confidentiality:

Our system is highly capable for providing confidentiality to the owner by encrypting his details on the device. Though the device is opened in another computer by providing password by the owner himself, he cannot view the details available on the device. This ensures data security. Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

II. Integrity:

Data integrity is defined as maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. Only if the owner wants to register a new account or wants to modify his personal details he can do so by providing the credentials on the device from his registered computer. The previous system has this disadvantage that the details can be modified by the owner from any system.

III. Availability:

The device is always available for use until and unless proper credentials are given to use it. The device quickly identifies the user by verifying the credentials from the local database. The device does evidence collection on wrong credentials or mismatch of device details.

IV. Non-repudiation:

The collected evidence can clearly state the status of the device whether it is being used by a legitimate user or by a thief. This information can be able to prove that the device has been stolen and it can support as an evidence for the crime. The existing system did not have any such feature. Device once stolen cannot be found nor can be tracked this drawback has been overcome by our system.

5. Conclusion and future enhancement

Our proposed system does have more security than the existing technology which prevails on the storage devices. The evidence collection which is the key concept of the proposed work helps improve security and gives a protection for the informations stored on the device. The existing system which just had data security was not that much secured because a good programmer or a hacker can decipher the data though it takes lots of days. When the data is deciphered the information which is contained in that becomes very valuable and it would cause a great impact on the individual or an organization which it is disclosed in public. So our proposed system added a tracking mechanism which does the monitoring of the device regularly whenever it is used. Our system collects important details like IP address, MAC address, USER Accounts details, OS Fingerprints etc., which is very unique and helpful to identify a computer. These details can act as one of the evidence in the court of law and this could be the starting point for further evidence and track the criminal and convicting the criminal for his act based on the Cyber laws and privacy preservation act.

The future enhancement of this system can add a GPS tracking chip with the device hardware so that the exact location of the device can be identified. Also a webserver could be maintained in addition to the software in the device so that remote handling the device like erasing the device, switching off the computer, sending a complaint automatically to a cyber-investigator etc.

Reference

[1] Mandaville K, Suman S, Thacker V, Ashwath Rao B "Theft detection of computers using MAC address by map-reduce programming model on a cluster", in *International Conference on Recent Advances in Computing and Software Systems (RACSS)*, 2012.

[2] Chuanxiong Guo ; Yunxin Liu ; Wenchao Shen ; Wang, H.J. "Mining the Web and the Internet for Accurate IP Address Geolocations", in *INFOCOM* , 2009.

[3]Shaobo Li, Zhisheng Shao, Shulin Lv, Xiaohui Jia, "The Design and implementation of Removable Storage Device Monitoring Based on WDM Filter Driver", in *International Symposium on Intelligence Information Processing and Trusted Computing (IPTC)*, 2010.

[4] http://en.wikipedia.org/wiki/Removable_media

[5] "The impact of mobile devices on information security: A survey of it professionals", *Dimensional Research*, 2012.

[6] Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, "Cyber security: challenges for society- literature review", in *IOSR Journal of Computer Engineering*, 2013.

[7] "The threats posed by portable storage devices", GFI Whitepapers.

[8] http://en.wikipedia.org/wiki/USB_flash_drive

[9] Pennie Walters, "The Risks of Using Portable Devices", US-CERT.

[10] IEEE Std. 802.11, IEEE Standards for Information Technology Telecommunications and Information Exchange between Systems Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[11] http://www.databreachtoday.asia/improving-security-for-usb-drives-a-5851